Belief Semantics of Authorization Logic

Andrew K. Hirsch and Michael R. Clarkson
Department of Computer Science
George Washington University
{akhirsch, clarkson}@gwu.edu

***Abstract*—A formal belief semantics is given for a constructive, first-order authorization logic. The belief semantics is proved to subsume a standard Kripke semantics. The belief semantics yields a direct representation of principals' beliefs, without resorting to the technical machinery used in Kripke semantics. A proof system is given for the logic; that system is proved sound with respect to the belief and Kripke semantics. The soundness proof for the Kripke semantics is mechanized in Coq.**

I. Introduction

Authorization logics are used in computer security to reason about whether *principals*—computer or human agents—are permitted to take actions in computer systems. The distinguishing feature of authorization logics is their use of a "says" connective: intuitively, if principal p believes that formula ϕ holds, then formula p says ϕ holds. Access control decisions can then be made by reasoning about (i) the beliefs of principals, (ii) how those beliefs can be combined to derive logical consequences, and (iii) whether those consequences entail *guard formulas*, which must hold for actions to be permitted.

Many systems that employ authorization logics have been proposed [1]–[18], but few authorization logics have been given a formal semantics [19]–[22]. Though semantics might not be immediately necessary to deploy authorization logics in real systems,

- semantics yield insight into the meaning of formulas, and
- semantics make it possible to prove the soundness of a proof system—which might require proof rules and axioms to be corrected, if there are any lurking errors in the proof system.

For the sake of security, it is worthwhile to carry out such soundness proofs. Given only a proof system, we must trust that the proof system is correct. But given a proof system and a soundness proof, which shows that any provable formula is semantically valid, we now have evidence that the proof system is correct, hence trustworthy. The soundness proof thus relocates trust from the proof system to the proof itself—as well as to the semantics, which ideally offers more intuition about formulas than the proof system itself.

The intuitive basis for semantics of epistemic logics is usually that of *possible worlds*, as used by Kripke [23]. Semantics that use this technique (henceforth, *Kripke semantics*) posit an indexed *accessibility relation* on possible worlds. If at world w, principal p considers world w' to be possible, then (w, w') is in p's accessibility relation. We denote this as $w \leq_p w'$. Authorization logics sometimes use Kripke semantics to give meaning to the says connective: semantically, p says ϕ holds in a world w iff for all worlds w' such that $w \leq_p w'$, formula ϕ holds in world w'. Hence a principal says ϕ iff ϕ holds in all worlds the principal considers possible.[1]

The use of Kripke semantics in authorization logic thus requires installation of possible worlds and accessibility relations into the semantics, solely to give meaning to says. Unfortunately, this approach does not seem to correspond to how principals reason in real-world systems. Rather than explicitly considering possible worlds and relations between them, principals typically begin with some set of base formulas they believe to hold—perhaps because they have received digitally signed messages encoding those formulas, or perhaps because they invoke system calls that return information—then proceed to reason from those formulas. So could we instead stipulate that each principal p have a set of beliefs $\omega(p)$, called the *worldview* of p, such that p says ϕ holds iff $\phi \in \omega(p)$? That is, a principal says ϕ iff ϕ is in the principal's worldview?

This paper answers that question in the affirmative. We give two semantics for an authorization logic: one semantics (§III) uses Kripke models, the other (§II) introduces *belief models*, which employ worldviews to interpret says.[2] We show (§IV) that belief models subsume Kripke models, in the sense that every Kripke model can be transformed into a belief model. If a formula is valid in the Kripke model, then it is also valid in the belief model. As a result, authorization logics can now eliminate the technical machinery of Kripke semantics and instead use *belief semantics*. This semantics potentially increases the trustworthiness of an authorization system, because the semantics is closer to how principals reason in real systems.

The particular logical system we introduce in this paper is FOCAL, First-Order Constructive Authorization Logic. FOCAL extends a well-known authorization logic, cut-down dependency core calculus (CDD) [28], from a propositional language to a language with first-order functions and relations on system state. Functions and relations are essential for reasoning about authorization in a real operating system—as exemplified in Nexus Authorization Logic (NAL) [29], of which FOCAL is a fragment. FOCAL also simplifies NAL by reducing from second-order to first-order quantification, with no important loss in expressivity.

[1] The says connective is, therefore, closely related to the modal necessity operator $\Box$ [24] and the epistemic knowledge operator K [25].

[2] Our belief models are an instance of the *syntactic* approach to modeling knowledge [25]–[27].

Having given two semantics for FOCAL, we then turn to the problem of proving soundness. It turns out that the NAL proof system is unsound w.r.t. the semantics presented here: NAL allows derivation of a formula our semantics considers invalid. A priori, the fault could lie with our semantics or with NAL's proof system. However, our examination of the formula (cf. §VI-D) suggests that if the logic is to be used in a distributed setting without globally-agreed upon state, then the proof system should not allow the formula to be derived. So if NAL is to be used in such settings, its proof system needs to be corrected.

NAL extends CDD, so CDD is also unsound w.r.t. our semantics. However, CDD has been proved sound w.r.t. a different semantics [21]. This seeming discrepancy—sound vs. unsound—illuminates a difference between how NAL and CDD interpret says. We discuss that difference in §VI-E.

To achieve soundness for FOCAL, we develop a revised proof system; the key technical change is adopting localized hypotheses in the proof rules. In §V, we prove the soundness of our proof system with respect to both our belief and Kripke semantics. This result yields the first soundness proof w.r.t. belief semantics for an authorization logic.

Having relocated trust into the soundness proof, we then seek a means to increase the trustworthiness of that proof. Accordingly, we formalize the syntax, proof system, and Kripke semantics in the Coq proof assistant,[3] and we mechanize the proof of soundness. That mechanization relocates trust from our soundness proof to the Coq proof system, which is well-studied and is the basis of many other formalizations. The full Coq formalization (including the formalization of FOCALE, discussed next) contains about 4,000 lines of code and required about four person-months for us, as Coq neophytes, to develop.[4] The mechanization effort was worthwhile in that it exposed various bugs in our semantics that might otherwise have remained unnoticed.

Finally, we extend FOCAL to include the advanced features found in NAL: restricted delegation, subprincipals, and intensional group principals (cf. §VI). These features, along with first-order functions and relations, can be used to implement the authorization system of an operating system built on a trusted platform module [18], and they enable rich reasoning about axiomatic, synthetic, and analytic bases for authorization of actions [29]. We call our extended logic FOCALE; it is quite similar to NAL, though there are some deliberate differences (cf. §VI). We give belief and Kripke semantics for FOCALE, give a proof system for FOCALE, and show the soundness of the proof system w.r.t. the belief semantics. We also show soundness w.r.t. the Kripke semantics and mechanize that proof in Coq. As a result, we obtain the first soundness proof for an authorization logic with intensional group principals.

We proceed as follows. §II presents FOCAL and its belief semantics. §III gives a Kripke semantics for FOCAL. §IV proves the relationship of the belief semantics to the Kripke semantics. §V gives a proof system for FOCAL and proves its soundness w.r.t. the Kripke semantics. §VI develops FOCALE by showing how to extend FOCAL's semantics and proof system to handle NAL's advanced features. §VII discusses related work, and §VIII concludes. All proofs appear in appendix A. Some familiarity with epistemic logics, constructive logics, and their Kripke semantics is assumed. Readers who seek background in these areas can consult standard references (e.g., [25], [30]).

$$\begin{array}{rl} \tau ::= & x \;\mid\; f(\tau,\ldots,\tau) \\ \phi ::= & \mathsf{true} \;\mid\; \mathsf{false} \;\mid\; r(\tau,\ldots,\tau) \;\mid\; \tau_1 = \tau_2 \\ & \mid\; \phi_1 \wedge \phi_2 \;\mid\; \phi_1 \vee \phi_2 \;\mid\; \phi_1 \Rightarrow \phi_2 \;\mid\; \neg\phi \\ & \mid\; (\forall\, x : \phi) \;\mid\; (\exists\, x : \phi) \\ & \mid\; \tau \;\mathsf{says}\; \phi \;\mid\; \tau_1 \;\mathsf{speaksfor}\; \tau_2 \end{array}$$

Fig. 1. Syntax of FOCAL

II. Belief Semantics

FOCAL is a constructive, first-order, multimodal logic. The key features that distinguish it as an authorization logic are the "says" and "speaks for" connectives, invented by Lampson et al. [1]. These are used to reason about authorization—for example, access control in a distributed system can be modeled in the following standard (albeit stylized) way:

Example 1. *A* guard *implements access control for a printer p. To permit printing to p, the guard must be convinced that guard formula $PrintServer$* says *$printTo(p)$ holds, where $PrintServer$ is the principal representing the server process. That formula means that $PrintServer$ believes $printTo(p)$ holds. To grant printer access to user u, the print server can issue the statement u* speaksfor *$PrintServer$. That formula means anything u says, the $PrintServer$ must also say. So if u* says *$printTo(p)$, then $PrintServer$* says *$printTo(p)$, which satisfies the guard formula hence affords the user access to the printer.*

Figure 1 gives the formal syntax of FOCAL. There are two syntactic classes, terms τ and formulas ϕ. Metavariable x ranges over first-order variables, f over first-order functions, and r over first-order relations.

Formulas of FOCAL do not permit monadic second-order universal quantification, unlike CDD and NAL. In NAL, which is an extension of CDD, that quantifier was used only to define false and speaksfor as syntactic sugar. FOCAL instead adds these as primitive connectives to the logic. This simplification reduces the logic from second-order down to first-order.

A. Semantic models

The belief semantics of FOCAL is based on a combination of two standard semantic models—first-order models and constructive models—with worldviews, which are used to interpret says and speaksfor. To our knowledge, this semantics is new in the study of authorization logics. Our presentation

[3] http://coq.inria.fr

[4] Our implementation is available from http://faculty.cs.gwu.edu/~clarkson/projects/focale/.

mostly follows the semantics of intuitionistic predicate calculus given by Troelstra and van Dalen [30].

First-order models: A *first-order model with equality* is a tuple $(D, =, R, F)$. The purpose of a first-order model is to interpret the first-order fragment of the logic, specifically first-order quantification, functions, and relations. D is a set, the *domain* of individuals. Semantically, quantification in the logic ranges over these individuals. R is a set $\{r_i \mid i \in I\}$ of relations on D, indexed by set I. Likewise, F is a set $\{f_j \mid j \in J\}$ of functions on D, indexed by set J. There is a distinguished equality relation $=$, which is an equivalence relation on D, such that equal individuals are indistinguishable by relations and functions.

To interpret first-order variables, the semantics employs *valuation* functions, which map variables to individuals. Denote the individual that variable x represents in valuation v as $v(x)$.

Constructive models: A *constructive model* is a tuple $(W, \leq, s)$. The purpose of constructive models is to extend first-order models to interpret the constructive fragment of the logic, specifically implication and universal quantification. W is a set, the *possible worlds*. We denote an individual world as w. Intuitively, a world w represents the *state of knowledge* of a constructive reasoner. *Constructive accessibility relation* $\leq$ is a partial order on W. If $w \leq w'$, then the constructive reasoner's state of knowledge could grow from w to w'. Function s is the *first-order interpretation function*. It assigns a first-order model $(D_w, =_w, R_w, F_w)$ to each world w. Let the individual elements of R_w be denoted $\{r_{i,w} \mid i \in I\}$; likewise for F_w, as $\{f_{j,w} \mid j \in J\}$. Thus, s enables a potentially different first-order interpretation at each world. But to help ensure that the constructive reasoner's state of knowledge only grows—hence never invalidates a previously admitted construction—we require s to be monotonic w.r.t. $\leq$. That is, if $w \leq w'$ then (i) $D_w \subseteq D_{w'}$, (ii) $d =_w d'$ implies $d =_{w'} d'$, (iii) $r_{i,w} \subseteq r_{i,w'}$, and (iv) for all tuples $\vec{d}$ of individuals, it holds that $f_{j,w}(\vec{d}) =_w f_{j,w'}(\vec{d})$.

It's natural to wonder why we chose to introduce possible worlds into the semantics here after arguing against them in §I. Note, though, that the worlds in the constructive model are being used to model only the constructive reasoner—which we might think of as the guard, who exists outside the logic and attempts to ascertain the truth of formulas—not any of the principals reasoned about inside the logic. Moreover, we have not introduced any accessibility relations for principals, but only a single accessibility relation for the constructive reasoner. So the arguments in §I don't apply here. It would be possible to eliminate our usage of possible worlds by employing a *Heyting algebra semantics* [31] of constructive logic. But possible worlds blend better with our eventual introduction of accessibility relations for principals in §III.

It's also natural to wonder why FOCAL is constructive rather than classical. Schneider et al. [29] write that constructivism preserves evidence: "Constructive logics are well suited for reasoning about authorization…because constructive proofs include all of the evidence used for reaching a conclusion and, therefore, information about accountability is not lost. Classical logics allow proofs that omit evidence." Garg and Pfenning [32] also champion the notion of evidence in authorization logics, writing that "[constructive logics] keep evidence contained in proofs as direct as possible." So we chose to make FOCAL constructive for the sake of evidence. Regardless, we believe that a classical version of FOCAL could be created without difficulty.

Belief models: A *belief model* is a tuple $(W, \leq, s, P, \omega)$. The purpose of belief models is to extend constructive models to interpret says and speaksfor. The first part of a belief model, $(W, \leq, s)$, must itself be a constructive model. The next part, P, is the set of principals. Although individuals can vary from world to world in a model, the set of principals is fixed across the entire model.[5] Because we make no syntactic distinction between individuals and principals, all principals must also be individuals: P must be a subset of D_w for every w. We define an equality relation $\doteq$ on principals, such that $p \doteq p'$ iff there exists a w such that $p =_w p'$.

The final part of a belief model, worldview function ω, yields the beliefs of a principal p: the set of formulas that p believes to hold in world w under valuation v is $\omega(w, p, v)$.[6] To ensure that the constructive reasoner's knowledge grows monotonically, worldviews must be monotonic w.r.t. $\leq$:

> **Worldview Monotonicity:** If $w \leq w'$ then $\omega(w, p, v) \subseteq \omega(w', p, v)$.

And to ensure that whenever principals are equal they have the same worldview, we require the following:

> **Principal Equality (Belief):** If $p \doteq p'$, then, for all w and v, it holds that $\omega(w, p, v) = \omega(w, p', v)$.

B. *Semantic validity*

Figure 2 gives a belief semantics of FOCAL. The validity judgment is written $B, w, v \models \phi$ where B is a belief model and w is a world in that model. As is standard, $B \models \phi$ holds iff, for all w and v, it holds that $B, w, v \models \phi$; whenever $B \models \phi$, then ϕ is a *necessary* formula in model B. And $B, v \models \phi$ holds iff for all w, it holds that $B, w, v \models \phi$; whenever $B, v \models \phi$, then ϕ is a *valuation-necessary* formula. Likewise, $\models \phi$ holds iff, for all B, it holds that $B \models \phi$; and whenever $\models \phi$, then ϕ is a *validity*. Finally, let $B, w, v \models \Gamma$, where Γ is a set of formulas, denote that for all $\psi \in \Gamma$, it holds that $B, w, v \models \psi$.

The semantics relies on an auxiliary *interpretation* function μ that maps syntactic terms τ to semantic individuals:

$$\mu(x) = v(x)$$
$$\mu(f_j(\vec{\tau})) = f_{j,w}(\mu(\vec{\tau}))$$

[5] This assumption is consistent with other constructive multimodal logics [33], [34], which have a fixed set of modalities (just $\Box$ and $\Diamond$), and with classical multimodal epistemic logics [25], which have an indexed set modalities (typically denoted K_i).

[6] For sake of simplicity, §I used notation $\omega(p)$ when first presenting the idea of worldviews. Now that we're being precise, ω needs two additional arguments: constructivity necessitates w, and first-orderedness necessitates v.

$$\begin{array}{lll}
B, w, v \models \mathsf{true} & & \text{always} \\
B, w, v \models \mathsf{false} & & \text{never} \\
B, w, v \models r_i(\vec{\tau}) & \text{iff} & \mu(\vec{\tau}) \in r_{i,w} \\
B, w, v \models \tau_1 = \tau_2 & \text{iff} & \mu(\tau_1) =_w \mu(\tau_2) \\
B, w, v \models \phi_1 \wedge \phi_2 & \text{iff} & B, w, v \models \phi_1 \text{ and } B, w, v \models \phi_2 \\
B, w, v \models \phi_1 \vee \phi_2 & \text{iff} & B, w, v \models \phi_1 \text{ or } B, w, v \models \phi_2 \\
B, w, v \models \phi_1 \Rightarrow \phi_2 & \text{iff} & \text{for all } w' \geq w : B, w', v \models \phi_1 \text{ implies } B, w', v \models \phi_2 \\
B, w, v \models \neg\phi & \text{iff} & \text{for all } w' \geq w : B, w', v \not\models \phi \\
B, w, v \models (\forall x : \phi) & \text{iff} & \text{for all } w' \geq w, d \in D_{w'} : B, w', v[d/x] \models \phi \\
B, w, v \models (\exists x : \phi) & \text{iff} & \text{there exists } d \in D_w : B, w, v[d/x] \models \phi \\
B, w, v \models \tau \;\mathsf{says}\; \phi & \text{iff} & \phi \in \omega(w, \mu(\tau), v) \\
B, w, v \models \tau_1 \;\mathsf{speaksfor}\; \tau_2 & \text{iff} & \omega(w, \mu(\tau_1), v) \subseteq \omega(w, \mu(\tau_2), v)
\end{array}$$

Fig. 2. FOCAL validity judgment for belief semantics

Implicitly, μ is parameterized on B, w, and v, but we omit writing these for notational simplicity.

The first-order, constructive fragment of the semantics is routine. The semantics of says is the intuitive semantics we wished for in §I: A principal $\mu(\tau)$ says ϕ exactly when ϕ is in that principal's worldview $\omega(w, \mu(\tau), v)$. And a principal $\mu(\tau_1)$ speaks for another principal $\mu(\tau_2)$ exactly when worldview $\omega(w, \mu(\tau_1), v)$ of $\mu(\tau_1)$ is a subset of worldview $\omega(w, \mu(\tau_2), v)$ of $\mu(\tau_2)$—hence everything $\mu(\tau_1)$ says, $\mu(\tau_2)$ also says.

Note that some syntactic terms may represent individuals that are not principals.[7] For example, the integer 42 is presumably not a principal in P, but it could be an individual in some domain D_w. Users of the logic could therefore write non-sensical formulas such as 42 says ϕ, assuming that 42 is a syntactic term. Such formulas would never hold semantically, because 42 does not have a worldview.

We impose a few *well-formedness* constraints on worldviews in this semantics, in addition to Worldview Monotonicity and Principal Equality (Belief). First, worldviews must be *deductively closed*—that is, principals must believe all the formulas that can be deduced from their beliefs. Let $\Gamma \vdash \phi$ denote that formula ϕ can be deduced from set Γ of formulas (we give a formal definition of relation $\vdash$ in §V):

> **Deductive Closure:** If $\Gamma \subseteq \omega(w, p, v)$ and $\Gamma \vdash \psi$, then $\psi \in \omega(w, p, v)$.

Deductive closure is closely related to *logical omniscience*, which, with its known benefits and flaws [35], [36], has been a standard assumption in authorization logics since their inception [1]. Although it might seem somewhat unusual to define this part of the semantics of FOCAL in terms of the proof system, it models our intuition that principals begin with a base set of beliefs and derive consequences.[8] NAL's [29] informal worldview semantics uses the same intuition.

Second, worldviews must ensure that says is a *transparent* modality—that is, for any principal p, it holds that p says ϕ exactly when p says $(p$ says $\phi)$:

> **Says Transparency:** $\phi \in \omega(w, \mu(\tau), v)$ iff $\tau \;\mathsf{says}\; \phi \in \omega(w, \mu(\tau), v)$.

So says supports *positive introspection*: if p believes that ϕ holds, then p is aware of that belief, therefore p believes that p believes that ϕ holds. Moreover, the converse of that holds as well. Recent authorization logics include transparency [29], [38], and it is well known (though sometimes vigorously debated) in epistemic logic [24], [39].

Third, worldviews must enable principals to delegate, or *hand-off*, to other principals: If a principal p believes that p' speaksfor p, it should hold that p' does speak for p:

> **Hand-off:** If $(\tau \;\mathsf{speaksfor}\; \tau') \in \omega(w, \mu(\tau'), v)$ then $\omega(w, \mu(\tau), v) \subseteq \omega(w, \mu(\tau'), v)$.

Hand-off, as the following axiom, existed in the earliest authorization logic [1], though not all logics since then have included it:

$$(\tau' \;\mathsf{says}\; (\tau \;\mathsf{speaksfor}\; \tau')) \Rightarrow (\tau \;\mathsf{speaksfor}\; \tau') \tag{1}$$

Each of these well-formedness conditions is necessary to achieve the soundness result of §V, because the proof system there includes rules that correspond to the conditions. But with appropriate changes to the proof system, any of the conditions could be eliminated.

III. Kripke Semantics

The Kripke semantics of FOCAL is a combination of three standard kinds of semantic models: first-order models, constructive models, and modal (Kripke) models. Similar semantic models have been explored before (see, e.g., [22], [33]), though we are not aware of any authorization logic semantics that is equivalent to or subsumes our semantics. First-order and constructive models were already presented in §II, so we begin here with modal models.

[7] We could make FOCAL a two-sorted logic, with one sort for individuals and another sort for principals. But having only a single sort is definitionally simpler. Another alternative would be to coerce individuals to principals—for example, treat 42 as the principal who believes only necessities (i.e., the $\perp$ principal defined in §VI).

[8] It would be possible to replace Deductive Closure with a purely semantic definition. But to maintain the results of §IV, the Kripke semantics of says in §III would need to be adjusted.

$$\begin{array}{lll}
K, w, v \models \tau \textsf{ says } \phi & \text{iff} & \text{for all } w', w'' : w \leq w' \leq_{\mu(\tau)} w'' \text{ implies } M, w'', v \models \phi \\
K, w, v \models \tau_1 \textsf{ speaksfor } \tau_2 & \text{iff} & \mathit{ReachAcc}(\mu(\tau_1), w) \supseteq \mathit{ReachAcc}(\mu(\tau_2), w) \\
K, w, v \models \ldots & \text{iff} & \textit{same as figure 2, but substituting K for B}
\end{array}$$

Fig. 3. FOCAL validity judgment for Kripke semantics

A. Modal models

A *modal model* is a tuple $(W, \leq, s, P, A)$. The purpose of a modal model is to extend constructive models to interpret says and speaksfor. The first part of a modal model, $(W, \leq, s)$, must itself be a constructive model. The next part, P, is the set of *principals*. As with belief models, all principals must be individuals, so P must be a subset of D_w for every w. Principal equality relation $\doteq$ is defined just as in belief models. The final part of a modal model, A, is a set $\{\leq_p \mid p \in P\}$ of binary relations on W, called the *principal accessibility relations*.[9] If $w \leq_p w'$, then at world w, principal p considers world w' possible. To ensure that equal principals have the same beliefs, we require

Principal Equality (Kripke): If $p \doteq p'$, then $\leq_p = \leq_{p'}$.

Like $\leq$ in a constructive model, we require s to be monotonic w.r.t. each $\leq_p$. This requirement enforces a kind of constructivity on each principal p, such that from a world in which individual d is constructed, p cannot consider possible any world in which d has not been constructed. Unlike $\leq$, none of the $\leq_p$ are required to be partial orders: they are not required to satisfy reflexivity, anti-symmetry, or transitivity.

That non-requirement raises an important question. In epistemic logics, the properties of what we call the "principal accessibility relations" determine what kind of knowledge is modeled [25]. If, for example, these relations must be reflexive, then the logic models *veridical* knowledge: if p says ϕ, then ϕ indeed holds. But that is not the kind of knowledge we seek to model with FOCAL, because principals may say things that in fact do not hold. So what are the right properties, or *frame conditions*, to require of our principal accessibility relations? We briefly delay presenting them, so that we can present the Kripke semantics.

B. Semantic validity

Figure 3 gives a Kripke semantics of FOCAL. The validity judgment is written $K, w, v \models \phi$ where K is a modal model and w is a world in that model. Only the judgments for the says and speaksfor connectives are given in figure 3. For the remaining connectives, the Kripke semantics is the same as the belief semantics in figure 2. Interpretation function μ remains unchanged from §II, except that it is now implicitly parameterized on K instead of B.

To understand the semantics of says, first observe the following. Suppose that, for all worlds w', it holds that $w \leq w'$ implies $w = w'$.[10] Then the semantics of says simplifies to

$$\begin{array}{l}
K, w, v \models \tau \textsf{ says } \phi \\
\qquad \text{iff} \quad \text{for all } w'' : w \leq_{\mu(\tau)} w'' \text{ implies } K, w, v \models \phi,
\end{array}$$

which is the standard semantics of $\Box$ in classical modal logic [24]: a principal believes a formula holds whenever that formula holds in all accessible worlds.

The purpose of the quantification over w', where $w \leq w'$, in the unsimplified semantics of says is to achieve *monotonicity* of the constructive reasoner:

Proposition 1. *If $K, w, v \models \phi$ and $w \leq w'$ then $K, w', v \models \phi$.*

That is, whenever ϕ holds at a world w, if the constructive reasoner is able to reach an extended state of knowledge at world w', then ϕ should continue to hold at w'. Without the quantification over w' in the semantics of says, monotonicity is not guaranteed to hold. Constructive modal logics have, unsurprisingly, also used this semantics for $\Box$ [33], [34].

Note that, if there do not exist any worlds w' and w'' such that $w \leq w' \leq_{\mu(\tau)} w''$, then at w, principal τ will say any formula ϕ, including false. When a principal says false at world w, we deem that principal *compromised* at w.

The semantics of speaksfor uses an auxiliary function $\mathit{ReachAcc}(p, w)$, which yields the component of $\leq_p$ that is reachable from, or reaches to, world w. Formally, let G_p be the undirected graph with nodes W and edges $\leq \cup \leq_p$. And let $[w]_p$ be the set of worlds w' such that w' and w are in the same connected component of G_p. Then $\mathit{ReachAcc}$ is defined as follows:[11]

$$\mathit{ReachAcc}(p, w) \triangleq \leq_p|_{[w]_p}.$$

So $\mathit{ReachAcc}(p, w)$ contains edge (w', w'') iff that edge is already present in $\leq_p$, and moreover w' and w'' are reachable from w by following any path that contains edges from either $\leq_p$ or $\leq$.

To understand the semantics of speaksfor, observe that whenever $[w]_p$ equals W, it holds that $\mathit{ReachAcc}(p, w)$ equals $\leq_p$. So the semantics simplifies to

$$K, w, v \models \tau_1 \textsf{ speaksfor } \tau_2 \quad \text{iff} \quad \leq_{\mu(\tau_1)} \supseteq \leq_{\mu(\tau_2)}. \tag{2}$$

That is, the accessibility relation of τ_1 must be a superset of the accessibility relation of τ_2. That definition is standard in classical authorization logics [19], [20].

[9] In our notation, an unsubscripted $\leq$ always denotes the constructive relation, and a subscripted $\leq$ always denotes a principal relation.

[10] This condition corresponds to the axiom of excluded middle, hence its imposition creates a classical variant of FOCAL. So it makes sense that adding the frame condition would result in the classical semantics of $\Box$.

[11] If R is a binary relation on set A, then $R|_X$ is the *restriction* of R to A, where $X \subseteq A$. That is, $R|_X = \{(x, x') \mid (x, x') \in R \text{ and } x \in X \text{ and } x' \in X\}$.

However, the classical definition has a surprising interaction with hand-off (1):

Example 2. *Consider a world w. Suppose there do not exist any worlds w' and w'' such that $w \leq w' \leq_{\mu(\tau)} w''$. Then at world w, principal τ is compromised: it says* false*, and also says any other formula ϕ.*

Let ϕ be τ' speaksfor *τ. Then it holds, for any principal τ', that $K, w, v \models \tau$* says *$(\tau'$* speaksfor *$\tau)$. By hand-off, we then have $K, w, v \models \tau'$* speaksfor *τ. By the classical semantics of* speaksfor*, we have $\leq_{\mu(\tau')} \supseteq \leq_{\mu(\tau)}$. So τ's accessibility relation must be a subset of all other principal's accessibility relations. In the extreme case, if there is a principal*[12] *whose accessibility relation is empty, τ's relation must also be empty.*

Therefore, if there ever is any world w at which principal τ is compromised, then τ's accessibility relation must be empty. That means if τ is compromised at one world, τ must be compromised at all worlds.

As a result, the constructive reasoner is immediately forced to recognize that a principal is compromised, even if the reasoner is in a minimal state of knowledge (i.e., at a world w at which there do not exist any worlds v such that $v \leq w$.) The reasoner is not allowed to wait until some greater state of knowledge to discover that a principal is compromised. This seems to be an intuitionistically undesirable feature.

We therefore relax the classical semantics of speaksfor by using $\mathit{ReachAcc}$:

$$\begin{aligned} &K, w, v \models \tau_1 \textsf{ speaksfor } \tau_2 \\ &\qquad \text{iff } \mathit{ReachAcc}(\mu(\tau_1), w) \supseteq \mathit{ReachAcc}(\mu(\tau_2), w) \quad (3) \end{aligned}$$

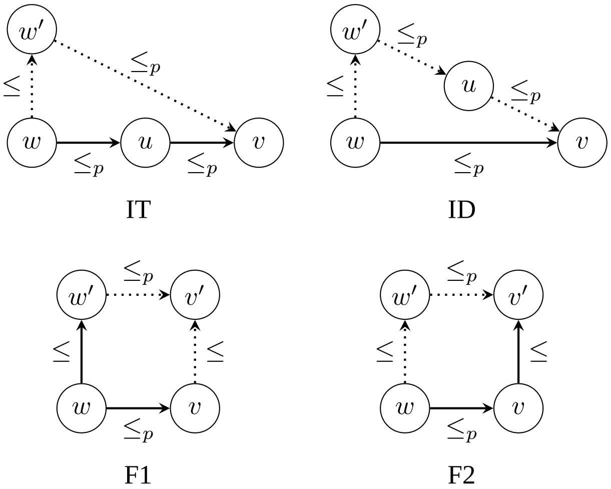
This is the semantics we adopt in FOCAL. With it, only the components of the accessibility relations that are locally reachable from w need to be considered. So a principal could be entirely compromised in some set of worlds not reachable from w, but that principal need not be compromised at w.

We've now seen two semantics of speaksfor (2), (3) that validate hand-off. That raises a question: what is the most permissive semantics of speaksfor (meaning that it allows as many models as possible) that validates hand-off? We don't know. One way to answer this question would be to show completeness of the FOCAL proof system. We leave that as future work.

C. Frame conditions

We now return to the discussion begun in §III-A of the frame conditions for FOCAL. The first two frame conditions we impose help to ensure Says Transparency.

> **IT:** If $w \leq_p u \leq_p v$, then there exists a w' such that $w \leq w' \leq_p v$.
>
> **ID:** If $w \leq_p v$, then there exists a w' and u such that $w \leq w' \leq_p u \leq_p v$.



IT

ID

F1

F2

Fig. 4. Frame conditions for Kripke semantics

Figure 4 depicts these conditions; dotted lines indicate existentially quantified edges. IT helps to guarantee if p says ϕ then p says $(p$ says $\phi)$; ID does the converse.[13]

Note how, if $w = w'$, the conditions reduce to the classical definitions of transitivity and density. Those classical conditions are exactly what guarantee transparency in classical modal logic.

IT and ID are not quite sufficient to yield transparency. But by also imposing the following frame condition, we do achieve transparency:[14]

> **F2:** If $w \leq_p v \leq v'$, then there exists a w' such that $w \leq w' \leq_p v'$.

F2 is depicted in figure 4. It is difficult to motivate F2 solely in terms of authorization logic, though it has been proposed in several Kripke semantics for constructive modal logics [34], [40]–[42]. But there are two reasons why F2 is desirable for FOCAL:

- Assuming F2 holds, IT and ID are not only sufficient but also necessary conditions for transparency—a result that follows from work by Plotkin and Stirling [40]. So in the presence of F2, transparency in FOCAL is precisely characterized by IT and ID.
- Suppose FOCAL were to be extended with a $\Diamond$ modality. It could be written τ suspects ϕ, with semantics $K, w, v \models \tau$ suspects ϕ iff there exists w' such that $w \leq_{\mu(\tau)} w'$ and $K, w', v \models \phi$. We would want says and suspects to interact smoothly. For example, it would be reasonable to expect that $\neg(\tau$ suspects $\phi)$ implies τ says $\neg\phi$. For if τ does not suspect ϕ holds anywhere, then τ should believe $\neg\phi$ holds. Condition F2 guarantees that implication [40]. So F2 prepares FOCAL for future

[12] We indeed will require the existence of such a principal, which we notate as $\top$, in §VI.

[13] IT and ID are abbreviations for intuitionistic transitivity and intuitionistic density. We use the term "intuitionistic" instead of "constructive" just to avoid confusion: CT might be read as classical or constructive transitivity.

[14] F2 is the name given this condition by Simpson [34].

extension with a suspects modality.[15]

Like the constraints imposed on worldviews in §II-B, IT, ID, and F2 are used to achieve the soundness result of §V. But with appropriate changes to the proof system, the frame conditions could be eliminated.

Finally, to ensure the validity of hand-off, we impose the following frame condition:

> **H:** For all principals p and worlds w, if there do not exist any worlds w' and w'' such that $w \leq w' \leq_p w''$, then, for all p', it must hold that $\mathit{ReachAcc}(p, w) \subseteq \mathit{ReachAcc}(p', w)$.

This condition guarantees that if a principal p becomes compromised at world w, then the reachable component of its accessibility relation will be a subset of all other principals'. By the FOCAL semantics of speaksfor, all other principals therefore speak for p at w, thus hand-off (1) from §II-B is valid.

IV. Semantic Transformation

We have now given two semantics for FOCAL, a belief semantics (§II) and a Kripke semantics (§III). Naturally, the question arises: how are these two semantics related? It turns out that the Kripke semantics can be soundly transformed into the belief semantics; but the Kripke semantics treats speaksfor differently than does the belief semantics—as we now explain.

Given a modal model K, there is a natural way to construct a belief model from it: assign each principal a worldview containing exactly the formulas that the principal says in K. Call this construction $\mathit{k2b}$, and let $\mathit{k2b}(K)$ denote the resulting belief model.

To give a precise definition of $\mathit{k2b}$, we need to introduce a new notation. Given semantic principal p, formula p says ϕ is not necessarily well-formed, because p is not necessarily a syntactic term. So let $K, w, v \models \hat{p}$ says ϕ be defined as follows: for all w' and w'' such that $w \leq w' \leq_p w''$, it holds that $K, w'', v \models \phi$. This definition simply unrolls the semantics of says to produce something well-formed.[16]

The precise definition of $\mathit{k2b}$ is as follows: if $K = (W, \leq, s, P, A)$, then $\mathit{k2b}(K)$ is belief model $(W, \leq, s, P, \omega)$, where $\omega(w, p, v)$ is defined to be $\{\phi \mid K, w, v \models \hat{p} \text{ says } \phi\}$.

Our first concern is whether $\mathit{k2b}(K)$ satisfies all the conditions required by §II: Worldview Monotonicity, Principal Equality (Belief), Deductive Closure, Says Transparency, and Hand-off. If a belief model B does satisfy these conditions, then B is *well-formed*. Construction $\mathit{k2b}$ does, indeed, produce well-formed belief models:

Proposition 2. *For all well-formed K, belief model $\mathit{k2b}(K)$ is well-formed.*

Modal model K is well-formed if it satisfies all the conditions required by §III: Principal Equality (Kripke), IT, ID, F2, and H.

Our second concern is whether $\mathit{k2b}(K)$ preserves the validity of formulas. In particular, if a formula is valid in K, it should remain so in $\mathit{k2b}(K)$. Construction $\mathit{k2b}$ does preserve validity:

Theorem 1. *For all K, w, v, and ϕ, if $K, w, v \models \phi$ then $\mathit{k2b}(K), w, v \models \phi$.*

The converse of theorem 1, however, does not hold. The problem is that some speaksfor formulas might be invalid in K yet become valid in $\mathit{k2b}(K)$. If, for example, principals p and q say all the same formulas in K, but their accessibility relations $\leq_p$ and $\leq_q$ are not the same, then they don't speak for each other in the Kripke semantics. Yet in $\mathit{k2b}(K)$, their worldviews will be equal, so they will speak for each other in the belief semantics.

This "feature" of the accessibility-relation based definition of speaksfor—that principals might not speak for each other yet have the same beliefs—is well-known. ABLP [19] and Howell [20] both identified definitions of speaksfor that would result in full equivalence of the belief and Kripke semantics of FOCAL; Howell calls this definition *weak speaks-for* and writes, "[O]ne may wonder why [ABLP] preferred a definition of speaks-for that was stronger than it needed to be. The intuition seems to be that [in A speaksfor B] the stronger semantics captures the fact that A understands B's reasons for believing various statements" [20, p. 43]. FOCAL adopts the stronger semantics of speaksfor for consistency with this prior work. Nonetheless, to obtain full equivalence of Kripke model to the constructed belief model, FOCAL could be modified to adopt the weak semantics.

We might wonder whether there is a construction that can soundly transform belief models into Kripke models. Consider trying to transform the following belief model B into a Kripke model:

> B has a single world w and a proposition (i.e., a nullary relation) X, such that, for all v, it holds that $B, w, v \not\models X$. Suppose that principal p's worldview contains X—i.e., for all v, it holds that $X \in \omega(w, p, v)$—and that p's worldview does not contain false. By the semantics of says, it holds that $B, w, v \models p$ says X.

When transforming B to a Kripke model K, what edges could we put in $\leq_p$? There are only two choices: $\leq_p$ could be empty, or $\leq_p$ could contain the single edge (w, w). If $\leq_p$ is empty, then p is compromised, hence p says false. That contradicts our assumption that false is not in p's worldview. If $w \leq_p w$, then for w' and w'' such that $w \leq w' \leq_p w''$, it does not hold that $K, w'', v \models \phi$—because w and w'' can only be instantiated as w, and $B, w, v \not\models X$. Hence p does not say X. That contradicts our assumption that X is in p's worldview. So we cannot

[15] Were suspects to be added to FOCAL, it would also be desirable to impose a fourth frame condition: if $w \leq w'$ and $w \leq_p v$, then there exists a v' such that $v \leq v'$ and $w' \leq_p v'$. This condition, named F1 by Simpson [34], guarantees [40] that τ suspects ϕ implies $\neg(\tau$ says $\neg\phi)$. It also guarantees monotonicity (cf. proposition 1) for suspects. Figure 4 depicts F1. Simpson [34, p. 51] argues that F1 and F2 could be seen as fundamental, not artificial, frame conditions for constructive modal logics.

[16] Another solution would be to stipulate that every principal p can be named by a term $\hat{p}$ in the syntax.

$$\frac{}{\Gamma, \phi \vdash \phi}\ \textsc{hyp} \qquad \frac{\Gamma \vdash \phi}{\Gamma, \psi \vdash \phi}\ \textsc{weak} \qquad \frac{}{\Gamma \vdash \mathsf{true}}\ \textsc{true-i} \qquad \frac{\Gamma \vdash \mathsf{false}}{\Gamma \vdash \phi}\ \textsc{false-e} \qquad \frac{\Gamma \vdash \phi \quad \Gamma \vdash \psi}{\Gamma \vdash \phi \wedge \psi}\ \textsc{and-i} \qquad \frac{\Gamma \vdash \phi \wedge \psi}{\Gamma \vdash \phi}\ \textsc{and-le}$$

$$\frac{\Gamma \vdash \phi \wedge \psi}{\Gamma \vdash \psi}\ \textsc{and-re} \qquad \frac{\Gamma \vdash \phi_1}{\Gamma \vdash \phi_1 \vee \phi_2}\ \textsc{or-li} \qquad \frac{\Gamma \vdash \phi_2}{\Gamma \vdash \phi_1 \vee \phi_2}\ \textsc{or-ri} \qquad \frac{\Gamma \vdash \phi_1 \vee \phi_2 \quad \Gamma, \phi_1 \vdash \psi \quad \Gamma, \phi_2 \vdash \psi}{\Gamma \vdash \psi}\ \textsc{or-e} \qquad \frac{\Gamma, \phi \vdash \psi}{\Gamma \vdash \phi \Rightarrow \psi}\ \textsc{imp-i}$$

$$\frac{\Gamma \vdash \phi \quad \Gamma \vdash \phi \Rightarrow \psi}{\Gamma \vdash \psi}\ \textsc{imp-e} \qquad \frac{\Gamma, \phi \vdash \mathsf{false}}{\Gamma \vdash \neg\phi}\ \textsc{not-i} \qquad \frac{\Gamma \vdash \phi \quad \Gamma \vdash \neg\phi}{\Gamma \vdash \mathsf{false}}\ \textsc{not-e} \qquad \frac{\Gamma \vdash \phi \quad x \notin FV(\Gamma)}{\Gamma \vdash (\forall x : \phi)}\ \textsc{forall-i} \qquad \frac{\Gamma \vdash (\forall x : \phi)}{\Gamma \vdash \phi[\tau/x]}\ \textsc{forall-e}$$

$$\frac{\Gamma \vdash \phi[\tau/x]}{\Gamma \vdash (\exists x : \phi)}\ \textsc{exists-i} \qquad \frac{\Gamma \vdash (\exists x : \phi) \quad \Gamma, \phi \vdash \psi \quad x \notin FV(\Gamma, \psi)}{\Gamma \vdash \psi}\ \textsc{exists-e} \qquad \frac{}{\Gamma \vdash \tau = \tau}\ \textsc{eq-r} \qquad \frac{\Gamma \vdash \tau_1 = \tau_2}{\Gamma \vdash \tau_2 = \tau_1}\ \textsc{eq-s}$$

$$\frac{\Gamma \vdash \tau_1 = \tau_2 \quad \Gamma \vdash \tau_2 = \tau_3}{\Gamma \vdash \tau_1 = \tau_3}\ \textsc{eq-t} \qquad \frac{\Gamma \vdash \tau_i = \tau_i'}{\Gamma \vdash f(\tau_1, \ldots, \tau_n) = f(\tau_1', \ldots, \tau_n')}\ \textsc{eq-f} \qquad \frac{\Gamma \vdash r(\tau_1, \ldots, \tau_n) \quad \Gamma \vdash \tau_i = \tau_i'}{\Gamma \vdash r(\tau_1', \ldots, \tau_n')}\ \textsc{eq-r}$$

$$\frac{\Gamma \vdash \phi}{\tau\ \mathsf{says}\ \Gamma \vdash \tau\ \mathsf{says}\ \phi}\ \textsc{says-lri} \qquad \frac{\Gamma \vdash \tau\ \mathsf{says}\ \phi}{\tau\ \mathsf{says}\ \Gamma \vdash \tau\ \mathsf{says}\ \phi}\ \textsc{says-li} \qquad \frac{\tau\ \mathsf{says}\ \Gamma \vdash \phi}{\tau\ \mathsf{says}\ \Gamma \vdash \tau\ \mathsf{says}\ \phi}\ \textsc{says-ri} \qquad \frac{\Gamma \vdash \tau_2\ \mathsf{says}\ (\tau_1\ \mathsf{speaksfor}\ \tau_2)}{\Gamma \vdash \tau_1\ \mathsf{speaksfor}\ \tau_2}\ \textsc{sf-i}$$

$$\frac{\Gamma \vdash \tau_1\ \mathsf{speaksfor}\ \tau_2 \quad \Gamma \vdash \tau_1\ \mathsf{says}\ \phi}{\Gamma \vdash \tau_2\ \mathsf{says}\ \phi}\ \textsc{sf-e} \qquad \frac{}{\Gamma \vdash \tau\ \mathsf{speaksfor}\ \tau}\ \textsc{sf-r} \qquad \frac{\Gamma \vdash \tau_1\ \mathsf{speaksfor}\ \tau_2 \quad \Gamma \vdash \tau_2\ \mathsf{speaksfor}\ \tau_3}{\Gamma \vdash \tau_1\ \mathsf{speaksfor}\ \tau_3}\ \textsc{sf-t}$$

Fig. 5. FOCAL derivability judgment

construct an accessibility relation $\leq_p$ that causes the resulting Kripke semantics to preserve validity of formulas from the belief semantics.

There is, therefore, no construction that can soundly transform belief models into Kripke models—unless, perhaps, the set of worlds is permitted to change. It might be possible to synthesize a new set of possible worlds, and equivalence relations on them, yielding a Kripke model that preserves validity of formulas from the belief model. We are investigating this possibility in ongoing work.

V. Proof System

FOCAL's derivability judgment is written $\Gamma \vdash \phi$ where Γ is a set of formulas called the *context*.[17] As is standard, we write $\vdash \phi$ when Γ is the empty set. In that case, ϕ is a *theorem*. We write Γ, ϕ to denote $\Gamma \cup \{\phi\}$.

Figure 5 presents the proof system. In it, $\phi[\tau/x]$ denotes capture-avoiding substitution of τ for x in ϕ. The first-order fragment of the proof system is routine (e.g., [43]–[45]). SAYS-LRI, SAYS-LI, and SAYS-RI use notation τ says Γ, which means that τ says all the formulas in set Γ. Formally, τ says Γ is defined as $\{\tau\ \mathsf{says}\ \phi \mid \phi \in \Gamma\}$.

SAYS-LRI corresponds [24] to standard axiom K from epistemic logic; SAYS-RI, to standard axiom 4; and SAYS-LI, to the converse $C4$ [38], [46] of 4:

$$\begin{aligned} K:&\quad (p\ \mathsf{says}\ (\phi \Rightarrow \psi)) \Rightarrow (p\ \mathsf{says}\ \phi) \Rightarrow (p\ \mathsf{says}\ \psi) \\ 4:&\quad (p\ \mathsf{says}\ \phi) \Rightarrow (p\ \mathsf{says}\ (p\ \mathsf{says}\ \phi)) \\ C4:&\quad (p\ \mathsf{says}\ (p\ \mathsf{says}\ \phi)) \Rightarrow (p\ \mathsf{says}\ \phi) \end{aligned}$$

K and SAYS-LRI mean that *modus ponens* applies inside says. They correspond to Deductive Closure. Because of SAYS-LRI and IMP-I, the deduction theorem holds for FOCAL [47]. $C4$ and 4, along with SAYS-LI and SAYS-RI, mean that p says (p says ϕ) is equivalent to p says ϕ; they correspond to Says Transparency. In the Kripke semantics, SAYS-RI corresponds to IT; and SAYS-LI, to ID.

SF-I corresponds to hand-off (1). SF-E uses speaksfor to deduce beliefs. SF-R and SF-T state that speaksfor is reflexive and transitive.

The usual sequent calculus structural rules of contraction, substitution and exchange are all admissible. But WEAK is not admissible: it must be directly included in the proof system, because the conclusions of SAYS-{LRI,LI,RI} capture their entire context Γ inside says.

Our first soundness theorem for FOCAL states that if ϕ is provable from assumptions Γ, and that if a belief model validates all the formulas in Γ, then that model must also validate ϕ. Therefore, any provable formula is valid in the belief semantics:

Theorem 2. *If $\Gamma \vdash \phi$ and $B, w, v \models \Gamma$, then $B, w, v \models \phi$.*

This result is, to our knowledge, the first proof of soundness for an authorization logic w.r.t. a belief semantics.

Our second soundness theorem for FOCAL states that any provable formula is valid in the Kripke semantics:

[17] These formulas are *localized hypotheses*, which the proof system uses instead of the hypothetical judgments found in natural deduction systems. Similar to the left-hand side Γ of a sequent $\Gamma \Longrightarrow \Delta$, the localized hypotheses are assumptions being used to derive right-hand side Δ. Unlike a sequent, Γ is a set, not a sequence.

Theorem 3. *If $\Gamma \vdash \phi$ and $K, w, v \models \Gamma$, then $K, w, v \models \phi$.*

We have mechanized the proof of theorem 3 in Coq. We expect that, with additional effort, the proof of theorem 2 could also be mechanized.

VI. Case Study: NAL

We now show how to extend FOCAL to a logic that we call FOCALE (for FOCAL Extended). FOCALE adds to FOCAL the connectives and features found in Nexus Authorization Logic (NAL) [29]—specifically, restricted delegation, subprincipals, and intensional group principals. Supporting these features requires non-trivial extensions to the semantic models of §II and §III. We chose to study NAL in part because it has been used to implement the authorization subsystem of a real operating system [18], which makes NAL a very practical authorization logic.

FOCALE extends the FOCAL syntax (figure 1) as follows:

$$\begin{array}{rl} \tau ::= & \ldots \mid \tau_1.\tau_2 \mid \{x : \phi\} \\ \phi ::= & \ldots \mid \tau_1 \ \mathsf{speaksfor}\ \tau_2 \ \mathsf{on}\ (x : \phi) \end{array}$$

These new syntactic forms are explained, next.

When a principal τ_2 is implemented by another principal τ_1, such that τ_1 can completely control τ_2's actions, then τ_2 is a *subprincipal* of τ_1, and τ_1 is a *superprincipal* of τ_2. That relationship is denoted $\tau_1.\tau_2$. For example, an operating system OS running on a CPU would be a subprincipal $CPU.OS$. And a process $proc$ executed by that operating system would be $(CPU.OS).proc$. Since τ_1 completely controls the actions of $\tau_1.\tau_2$, anything τ_1 believes is also a belief of $\tau_1.\tau_2$.

An *intensional group principal* is a principal whose beliefs are an aggregation of the beliefs of other principals. It is "intensional" because it is defined by a characteristic predicate: group $\{x : \phi\}$ is the principal whose beliefs are the aggregation of the beliefs of all principals x who satisfy formula ϕ, where x is free in ϕ. *Aggregation* in NAL, hence in FOCALE, means union followed by deductive closure. So groups are *disjunctive*.[18] For example, formula ϕ is a belief of group $\{x : x = Alice \vee x = Bob\}$ if ϕ is a belief of $Alice$, or is a belief of Bob, or can be deduced from the union of the beliefs of $Alice$ and Bob. Because of group principals, terms and formulas are now mutually recursive syntactic classes.

Finally, *restricted delegation* is a limited form of speaksfor in which a principal delegates only partial authority to another principal. When τ_1 speaksfor τ_2 on $(x : \phi)$, only on statements ϕ with free variable x does τ_1 speak for τ_2:

Example 3. *If u speaksfor $PrintServer$ on $(p : printTo(p))$, then whenever user u says $printTo(labPrinter)$, it will be as if $PrintServer$ says $printTo(labPrinter)$. But if u says a formula ψ not of the form $(p : printTo(p))$—for example, u says $emptyPrintQueue(labPrinter)$—then it will not be as if $PrintServer$ says ψ.*

A. FOCALE belief semantics

A *FOCALE belief model* is a tuple $(W, \leq, s, P, \omega, \sqcup, \bot, \top)$. The first part of a FOCALE belief model, $(W, \leq, s, P, \omega)$, must be a belief model as in §II-A. The remaining parts of the model are used to interpret group and subprincipals.

To interpret group principals, we now require set P of principals to form a join semilattice under join operation $\sqcup$. The lattice must have a bottom element $\bot$ and top element $\top$. Principal $\top$ believes every formula, including false, whereas principal $\bot$ believes only valuation necessities (cf. §II-B). Join operator $\sqcup$ is used to take disjunctions of principals: $p \sqcup q$ is the principal who believes those statements that either p or q believe, or statements that can be deduced from those. Formally, we require that the following condition holds:

> **Group Principal (Belief):** For all principals p and q, and for all w and v, worldview $\omega(w, (p \sqcup q), v)$ is the deductive closure of $\omega(w, p, v) \cup \omega(w, q, v)$.

To interpret subprincipals, we now require the existence of a distinguished first-order function sub_w at each world w. Given principal p and individual d, function $sub_w(p, d)$ yields the principal q that corresponds to d as implemented by p. For all p and d, we require that $\omega(p) \subseteq \omega(sub_w(p, d))$ holds, so that subprincipals are guaranteed to believe any formula believed by a superprincipal.

Interpretation function μ is now extended to handle subprincipals and group principals:

$$\begin{aligned} \mu(\tau_1.\tau_2) \quad &= sub_w(\mu(\tau_1), \mu(\tau_2)) \\ \mu(\{x : \phi\}) &= \bigsqcup_{p \,:\, B,w,v[p/x] \models \phi} p \end{aligned}$$

As in §II, function μ is implicitly parameterized on B, w, and v. The interpretation of subprincipals is straightforward: simply interpret each term individually, then use sub_w to yield the subprincipal. Group principals are interpreted by taking the join over all principals p who satisfy formula ϕ. If no principal satisfies ϕ, the result of the empty join is $\bot$.

The semantics of restricted delegation is a simple adaptation of the semantics in figure 2:

$$\begin{aligned} &B, w, v \models \tau_1 \ \mathsf{speaksfor}\ \tau_2 \ \mathsf{on}\ (x : \phi) \\ &\qquad \text{iff} \quad \omega(w, \mu(\tau_1), v) \cap S \subseteq \omega(w, \mu(\tau_2), v) \cap S, \end{aligned}$$

where $S = \{\phi[\tau/x] \mid \tau\}$. That is, the worldview of τ_1 must be a subset of the worldview of τ_2, but only on formulas of the form ϕ.

B. FOCALE Kripke semantics

A *FOCALE modal model* is a tuple $(W, \leq, s, P, A, \sqcup, \bot, \top)$. The first part of a FOCALE modal model, $(W, \leq, s, P, A)$, must be a modal model as in §III-A. As with FOCALE belief models, P must form a join semilattice under $\sqcup$. The intuitive interpretation of this lattice remains unchanged, but we replace condition Group Principal (Belief) with the following condition:

> **Group Principal (Kripke):** For all principals p and q, it holds that $A_{p \sqcup q} = A_p \cap A_q$.

[18] There would be no problem defining *conjunctive* groups based on intersection of beliefs, but NAL does not include them so neither does FOCALE.

$$\frac{\Gamma \vdash \tau_2 \;\mathsf{says}\; (\tau_1 \;\mathsf{speaksfor}\; \tau_2 \;\mathsf{on}\; (x:\phi))}{\Gamma \vdash \tau_1 \;\mathsf{speaksfor}\; \tau_2 \;\mathsf{on}\; (x:\phi)}\ \textsc{rsf-i} \qquad \frac{\Gamma \vdash \tau_1 \;\mathsf{speaksfor}\; \tau_2 \;\mathsf{on}\; (x:\phi) \quad \Gamma \vdash \tau_1 \;\mathsf{says}\; \phi[\tau/x]}{\Gamma \vdash \tau_2 \;\mathsf{says}\; \phi[\tau/x]}\ \textsc{rsf-e}$$

$$\frac{}{\Gamma \vdash \tau \;\mathsf{speaksfor}\; \tau \;\mathsf{on}\; (x:\phi)}\ \textsc{rsf-r} \qquad \frac{\Gamma \vdash \tau_1 \;\mathsf{speaksfor}\; \tau_2 \;\mathsf{on}\; (x:\phi) \quad \Gamma \vdash \tau_2 \;\mathsf{speaksfor}\; \tau_3 \;\mathsf{on}\; (x:\phi)}{\Gamma \vdash \tau_1 \;\mathsf{speaksfor}\; \tau_3 \;\mathsf{on}\; (x:\phi)}\ \textsc{rsf-t}$$

$$\frac{\Gamma \vdash \phi[\tau/x]}{\Gamma \vdash \tau \;\mathsf{speaksfor}\; \{x:\phi\}}\ \textsc{member} \qquad \frac{\Gamma, \phi \vdash x \;\mathsf{speaksfor}\; \tau \quad x \notin FV(\tau) \cup FV(\Gamma)}{\Gamma \vdash \{x:\phi\} \;\mathsf{speaksfor}\; \tau}\ \textsc{sf-group} \qquad \frac{}{\Gamma \vdash \tau_1 \;\mathsf{speaksfor}\; \tau_1.\tau_2}\ \textsc{sf-subprin}$$

Fig. 6. FOCALE derivability judgment

Top principal $\top$ has the empty accessibility relation—that is, $A_\top = \emptyset$—which means that $\top$ believes every formula. And bottom principal $\bot$ has the complete accessibility relation—that is, $A_\bot = W \times W$—which means that $\bot$ believes only valuation necessities (cf. §II-B).

Interpretation function μ is extended to handle subprincipals and group principals. To interpret subprincipals, we again require the existence of sub_w at each world w, with the same intuitive meaning as before. Formally, for all p, d, and w, we now require that $A_p \supseteq A_{sub_w(p,d)}$. This requirement ensures that subprincipals believe any formula believed by a superprincipal. When interpreting group principals, the join is now taken over all principals p such that $K, w, v[p/x] \models \phi$ holds. This interpretation is similar to the algebra of principals defined in ABLP logic [19].

The semantics of restricted delegation is more complicated, and resembles a semantics invented by Howell [20]:

$$\begin{aligned} &K, w, v \models \tau_1 \;\mathsf{speaksfor}\; \tau_2 \;\mathsf{on}\; (x:\phi) \\ &\qquad \text{iff for all } w', w'' : (w', w'') \in A_{\mu(\tau_2)} \\ &\qquad\qquad \text{implies there exists } w''' : w'' \equiv^{w'}_{x:\phi} w''' \\ &\qquad\qquad\qquad \text{and } (w', w''') \in A_{\mu(\tau_1)} \end{aligned}$$

To understand this definition, first notice its use of an equivalence relation $\equiv^w_{x:\phi}$ on worlds. (We briefly postpone defining that relation.) Suppose, for sake of explanation, that we replaced the equivalence relation with simple equality of worlds. Then the semantics would require (in the third line) that $w'' = w'''$, in which case it would simplify to

$$\begin{aligned} \text{for all } w', w'' \ :\ & (w', w'') \in A_{\mu(\tau_2)} \\ & \text{implies } (w', w'') \in A_{\mu(\tau_1)}, \end{aligned}$$

which itself simplifies to $A_{\mu(\tau_2)} \subseteq A_{\mu(\tau_1)}$. That is exactly the semantics of *unrestricted* delegation $\tau_1 \;\mathsf{speaksfor}\; \tau_2$. So the generalization of equality to equivalence is the only new aspect of the semantics of restricted delegation.

Intuitively, equivalence relation $\equiv^w_{x:\phi}$ deems two worlds to be equivalent if they agree on the validity of formula ϕ in all valuations, assuming the existence of individuals D_w. Formally, define $w' \equiv^w_{x:\phi} w''$ to hold iff

$$\begin{aligned} \forall d \in D_w : \forall v : \quad & (M, w', v[d/x] \models \phi) \\ & \iff (M, w'', v[d/x] \models \phi). \end{aligned}$$

Returning to the (unsimplified) semantics of restricted delegation, note it requires that for any edge (w', w'') in τ_2's accessibility relation, there must also be any edge (w', w''') in τ_1's accessibility relation, such that w'' and w''' agree on the validity of ϕ. That guarantees whenever $\tau_1 \;\mathsf{says}\; \phi[\tau/x]$ holds, $\tau_2 \;\mathsf{says}\; \phi[\tau/x]$ also holds, because the worlds that are accessible to τ_2 agree on the validity of ϕ with the worlds that are accessible to τ_1.

We believe that the results relating the FOCAL belief and Kripke semantics (§IV) could be extended to FOCALE.

C. FOCALE proof system

The FOCALE proof system contains all the FOCAL proof rules (figure 5) as well as the additional rules in figure 6. Restricted delegation rules RSF-I, RSF-E, RSF-R, and RSF-T are straightforward adaptations of the rules for unrestricted delegation. Rules MEMBER, SF-GROUP, and SF-SUBPRIN are adaptations of the NAL rules [29] for group principals and subprincipals.[19]

The soundness theorems for FOCALE are as follows:

Theorem 4. *If $\Gamma \vdash \phi$ and $B, w, v \models \Gamma$, then $B, w, v \models \phi$.*

Theorem 5. *If $\Gamma \vdash \phi$ and $K, w, v \models \Gamma$, then $K, w, v \models \phi$.*

We have mechanized the proof of theorem 5 in Coq. (We expect that, with additional effort, the proof of theorem 4 could also be mechanized.) The mechanized proof contains about 4,000 lines, as measured by `wc -l`. It currently uses two additional axioms about the interpretation of principals:

1) If the interpretation of a term τ at a world w is individual d, then future worlds w' must also interpret τ as d. So, informally, the interpretation of terms can't change between worlds. Formally, let $\mu_w(\tau)$ denote the application of μ to term τ in world w. Formally, for all τ, w and w', if $w \leq w'$, or if there a exists p such that $w \leq_p w'$, then it must hold that $\mu_w(\tau) = \mu_{w'}(\tau)$. This axiom is actually provable as a theorem for all terms except group principals.
2) If the interpretation of a term at a world is principal p, then all other worlds must interpret that term as a principal equivalent to p. So a term must always be

[19] NAL's group monotonicity rule is a derived rule in the NAL proof system, and it is also a derived rule of the FOCALE proof system. We omit it here.

interpreted as the same principal. Formally, for all τ and w, if $\mu_w(\tau) \in P$ then, for all w', it must hold that $\mu_{w'}(\tau) \in P$ and $\mu_w(\tau) \doteq \mu_{w'}(\tau)$.

In ongoing work, we are attempting to eliminate these axioms.

D. FOCALE vs. NAL

FOCALE has essentially the same proof system as NAL, but there are a few differences:

- NAL has second-order universal monadic quantification. But it uses that feature only to define speaksfor and false as derived forms; it was never otherwise needed in the examples in the NAL rationale [29]. So FOCALE eliminates it and enjoys a simpler, first-order semantics.[20]
- NAL's term language, including principals, was not fully specified. FOCALE provides a full syntax, semantics, and proof system that we believe is consistent with the examples in the NAL rationale [29].
- The NAL proof system is a natural deduction style system with hypothetical judgments. The FOCALE proof system instead uses localized hypotheses, which we found easy to work with when mechanizing the proof system in Coq.

Finally, we deliberately designed the FOCALE proof system such that its theory differs in one important way from NAL's. We discuss our motivation for this change, next.

There are two standard ways of "importing" beliefs into a principal's worldview. The first is a rule known as Necessitation:

$$\frac{\vdash \phi}{\vdash p \ \mathsf{says}\ \phi}$$

The second is an axiom known as Unit:

$$\vdash \phi \Rightarrow (p \ \mathsf{says}\ \phi)$$

Though superficially similar, Necessitation and Unit lead to different theories.

Example 4. *Machines M_1 and M_2 execute processes P_1 and P_2, respectively. M_1 has a register R. Let Z be a proposition representing "register R is currently set to zero." According to Unit, $\vdash Z \Rightarrow (P_1 \ \mathsf{says}\ Z)$ and $\vdash Z \Rightarrow (P_2 \ \mathsf{says}\ Z)$. The former means that a process on a machine knows the current contents of a register on that machine; the latter means that a process on a different machine must also know the current contents of the register. But according to Necessitation, if $\vdash Z$ then $\vdash P_1 \ \mathsf{says}\ Z$ and $\vdash P_2 \ \mathsf{says}\ Z$. Only if R is always zero must the two processes say so.*

Unit, therefore, is appropriate when propositions (or relations or functions) represent global state upon which all principals are guaranteed to agree. But when propositions represent local state that could be unknown to some principals, Unit would arguably be an invalid axiom. A countermodel demonstrating its invalidity is easy to construct—for example, stipulate a world w at which Z holds, and let P_1's worldview contain Z but P_2's worldview not contain Z.

FOCALE was designed to reason about state in distributed systems, where principals (such as machines) may have local state, and where global state does not necessarily exist—the reading at a clock, for example, is not agreed upon by all principals. So Unit would be invalid for FOCALE principals; Necessitation is the appropriate choice.

Similarly, NAL principals do not necessarily agree upon global state. NAL does include Necessitation as an inference rule and does not include Unit as an axiom. However, NAL permits Unit to be derived as a theorem by the following proof:[21]

$$\cfrac{\cfrac{[\phi]^1}{p \ \mathsf{says}\ \phi}\ \textsc{nal-says-i}}{\phi \Rightarrow p \ \mathsf{says}\ \phi}\ \textsc{nal-imp-i}_1$$

NAL's proof system is, therefore, arguably unsound w.r.t. the belief semantics presented here: there is a formula (Unit) that is a theorem of the system but that is not semantically valid.

One way to remedy NAL's unsoundness w.r.t. our semantics would be to adjust our semantics, such that Unit becomes valid:

> **U1:** In our belief semantics, require that whenever $w \models \phi$, it must hold that $\phi \in \omega(w, p, v)$.[22]

(An equivalent condition could be imposed on the Kripke semantics.) But we chose not to do this because we want to model principals who may be ignorant of whether certain facts hold at a world. Indeed, in our semantics, if ϕ holds at a world, some principals might believe ϕ at that world and some might not. The adjustments above would instead cause all principals to believe ϕ at the world, and we find this to be an unacceptable loss in expressivity.

Another way to remedy NAL's unsoundness w.r.t. our semantics would be to adjust NAL's proof system, such that Unit is no longer derivable. For example, a side-condition could be added to NAL-SAYS-I, such that ϕ must be a validity.[23] One way of accomplishing that might be to forbid uncancelled hypotheses in the derivation of ϕ. That would prevent the above derivation of Unit, although we don't know what effect it would have on the completeness of the proof system.

FOCALE's proof system (specifically, rule SAYS-LRI) instead prohibits derivation of Unit: Unit is invalid in our semantics, and our proof system is sound w.r.t. our semantics, so it's impossible for our proof system to derive Unit. FOCALE therefore seems appropriate for reasoning about state in distributed systems.

[20] Garg and Abadi [21] show that the second-order definition of speaksfor likewise can be eliminated in the logic ICL, which is related to CDD hence to NAL.

[21] Rules NAL-IMP-I and NAL-SAYS-I can be found in [29]. The brackets around ϕ at the top of the proof tree indicate that it is used as a hypothesis [44]. The appearance of "1" as a super- and subscript indicate where the hypothesis is introduced and cancelled.

[22] U1 was omitted from the NAL rational [29]. But for the NAL proof system to be sound w.r.t. the informal NAL belief semantics, the condition should have been imposed.

[23] Fred B. Schneider, personal communication, January 31, 2013.

E. FOCALE vs. CDD

NAL extends CDD's proof system [28], so we might suspect that CDD is also unsound w.r.t. our semantics. And it is. However, CDD has been proved sound w.r.t. a *lax logic* semantics [21]. That semantics employs a different intuition about says than NAL and FOCALE. CDD [28, p. 13] understands p says ϕ to mean "when combining the [statement ϕ] that the [guard] believes with those that [p] contributes, the [guard] can conclude ϕ. . . the [guard's] participation is left implicit." In other words, the guard's beliefs are imported into p's beliefs at each world. That's equivalent to our condition U1 above, and it results in a different meaning of says than FOCALE or NAL employs.

VII. Related Work

FOCAL has the first formal belief semantics of any authorization logic. To our knowledge, belief semantics have been used in only one other authorization logic, and that logic—NAL [29]—has only an informal semantics. Semantic structures similar to our belief models have been investigated in the context of epistemic logic [26], [27]. Fagin et al. [25] call them *syntactic* models, and Konolige [37] calls them *deduction models*. Konolige proves the equivalence of deduction models and Kripke models for classical propositional logic.

Garg and Abadi [21] give a Kripke semantics for a logic they call ICL, which could be regarded as the propositional fragment of FOCAL. The ICL semantics of says, however, uses *invisible* worlds to permit principals to be oblivious to the truth of formulas at some worlds. That makes Unit (§VI-D) valid in ICL, whereas Unit is invalid in FOCAL.

Genovese et al. [22] study several uses for Kripke semantics with an authorization logic they call $\mathrm{BL}_{\mathrm{sf}}$, which also could be regarded as the propositional fragment of FOCAL. Using their Kripke semantics, they show how to generate evidence for why an access should be denied, how to find all logical consequences of an authorization policy, and how to determine which additional credentials would allow an access. These questions would also be interesting to address in FOCAL. However, the Kripke semantics of $\mathrm{BL}_{\mathrm{sf}}$ differs from FOCAL's in its interpretation of both says and speaksfor, so the results of Genovese et al. are not immediately applicable to FOCAL.

Garg and Pfenning [32] prove *non-interference* properties for a first-order, constructive authorization logic. Roughly speaking, these properties mean that one principal's beliefs cannot interfere with another principal's beliefs unless there is some trust relationship between those principals. Abadi [28] also proves such a property for dependency core calculus (DCC), which is the basis of authorization logic CDD. We believe that similar properties could be proved for FOCAL.

Garg and Pfenning [48] reject Unit in their authorization logic BL_0, as we did in FOCAL. They demonstrate that Unit leads to counterintuitive interpretations of some formulas involving delegation. Abadi [38] notes that Unit "should be used with caution (if at all)," and suggests replacing it with the weaker axiom $(p \textsf{ says } \phi) \Rightarrow (q \textsf{ says } p \textsf{ says } \phi)$. Genovese et al. [22] adopt that axiom; in their Kripke semantics, the frame condition that validates it is: $w \leq_p u \leq_q v$ implies $w \leq_q v$. That condition could be added to FOCAL.

VIII. Concluding Remarks

This work began with the idea of giving a Kripke semantics to NAL. Proving soundness—at first on paper, not in Coq—turned out to be surprising, because Unit is semantically invalid but derivable in NAL (§VI-D). As we continued proving soundness, we (re)discovered the need to impose frame conditions on the two kinds of accessibility relations involved in the Kripke semantics (§III-C). The complexity of the resulting Kripke semantics motivated us to seek a simpler semantics. We were inspired by the informal semantics of the NAL rationale [29] and elaborated that into our belief semantics (§II).

Mechanizing the proof of soundness in Coq was frequently rewarding. Even though it took a fair amount of effort, it exposed several bugs (in either our proof system or our semantics) and gave us high confidence in the correctness of the result. We expect future benefits, too. From the formalization of the FOCALE proof system in Coq, we could next extract a *verified theorem checker*. It would input a proof of a FOCALE formula, expressed in the FOCALE proof system, and output whether the proof is correct. Coq would verify that the checker correctly implements the FOCALE proof system. This theorem checker could replace the current Nexus [18] theorem checker, which is implemented in C.[24] A verified theorem checker would arguably be more trustworthy than the C implementation, thus increasing the trustworthiness of the operating system.

One of the more intriguing consequences of our semantics is that says is not a *monad* [49]. Since Abadi's invention of CDD [28], says is frequently assumed to satisfy the *monad laws*, which include Unit.[25] In our semantics, however, Unit is invalid, and we've argued here that it is inappropriate for distributed systems. We don't know whether rejecting the monad laws will have any practical impact on FOCAL. But the seminal authorization logic, ABLP [19], didn't adopt the monad laws, so at least FOCAL is in good company.

Acknowledgments

Fred B. Schneider consulted on the design of the proof system and the Kripke semantics. We thank him, Martín Abadi, Deepak Garg, Joe Halpern, Dexter Kozen, Colin Stirling, and Kevin Walsh for discussions related to this work. We also thank Adam Chlipala, Kristopher Micinski, and the coq-club mailing list for assistance with Coq. This work was supported in part by AFOSR grants F9550-06-0019, FA9550-11-1-0137, and FA9550-12-1-0334, NSF grants 0430161, 0964409, and CCF-0424422 (TRUST), ONR grants N00014-01-1-0968 and N00014-09-1-0652, and a grant from Microsoft.

[24] Nexus would have to be modified to use the FOCALE proof system rather than the NAL proof system for this replacement to succeed.

[25] The monad laws also include a law named Bind, which turns out to be semantically invalid in our semantics as well.

REFERENCES

[1] B. Lampson, M. Abadi, M. Burrows, and E. Wobber, "Authentication in distributed systems: Theory and practice," *ACM Transactions on Computer Systems*, vol. 10, no. 4, pp. 265–310, Nov. 1992.

[2] E. Wobber, M. Abadi, M. Burrows, and B. Lampson, "Authentication in the Taos operating system," *ACM Transactions on Computer Systems*, vol. 12, no. 1, pp. 3–32, Feb. 1994.

[3] A. W. Appel and E. W. Felten, "Proof-carrying authentication," in *Proc. ACM Conference on Computer and Communications Security (CCS)*, 1999, pp. 52–62.

[4] N. Li, B. N. Grosof, and J. Feigenbaum, "A practically implementable and tractable delegation logic," in *IEEE Symposium on Security and Privacy*, 2000, pp. 27–42.

[5] T. Jim, "SD3: A trust management system with certified evaluation," in *IEEE Symposium on Security and Privacy*, 2001, pp. 106–115.

[6] J. DeTreville, "Binder, a logic-based security language," in *IEEE Symposium on Security and Privacy*, 2002, pp. 105–113.

[7] N. Li, J. C. Mitchell, and W. H. Winsborough, "Design of a role-based trust-management framework," in *IEEE Symposium on Security and Privacy*, 2002, pp. 114–130.

[8] M. Y. Becker and P. Sewell, "Cassandra: Distributed access control policies with tunable expressiveness," in *Proc. IEEE Workshop on Policies for Distributed Systems and Networks (POLICY)*, 2004, pp. 159–168.

[9] L. Bauer, S. Garriss, J. M. McCune, M. K. Reiter, J. Rouse, and P. Rutenbar, "Device-enabled authorization in the Grey system," in *Proc. Information Security Conference (ISC)*, 2005, pp. 431–445.

[10] C. Fournet, A. D. Gordon, and S. Maffeis, "A type discipline for authorization policies," in *Proc. European Symposium on Programming (ESOP)*, 2005, pp. 141–156.

[11] A. Pimlott and O. Kiselyov, "Soutei, a logic-based trust-management system," in *Proc. Functional and Logic Programming Symposium (FLOPS)*, 2006, pp. 130–145.

[12] J. G. Cederquist, R. Corin, M. A. C. Dekker, S. Etalle, J. I. den Hartog, and G. Lenzini, "Audit-based compliance control," *Int'l Journal of Information Security*, vol. 6, no. 2–3, pp. 133–151, 2007.

[13] A. Cirillo, R. Jagadeesan, C. Pitcher, and J. Riely, "Do As I SaY! Programmatic access control with explicit identities," in *Proc. IEEE Computer Security Foundations Symposium (CSF)*, 2007, pp. 16–30.

[14] C. Lesniewski-Laas, B. Ford, J. Strauss, R. Morris, and M. F. Kaashoek, "Alpaca: extensible authorization for distributed services," in *Proc. ACM Conference on Computer and Communications Security (CCS)*, 2007, pp. 432–444.

[15] Y. Gurevich and I. Neeman, "DKAL: Distributed-knowledge authorization language," in *Proc. IEEE Computer Security Foundations Symposium (CSF)*, 2008, pp. 149–162.

[16] L. Jia, J. A. Vaughan, K. Mazurak, J. Zhao, L. Zarko, J. Schorr, and S. Zdancewic, "AURA: A programming language for authorization and audit," in *Proc. ACM Int'l Conference on Functional Programming (ICFP)*, 2008, pp. 27–38.

[17] M. Y. Becker, C. Fournet, and A. D. Gordon, "SecPAL: Design and semantics of a decentralized authorization language," *Journal of Computer Security*, vol. 18, no. 4, pp. 619–665, 2010.

[18] E. G. Sirer, W. de Bruijn, P. Reynolds, A. Shieh, K. Walsh, D. Williams, and F. B. Schneider, "Logical attestation: An authorization architecture for trustworthy computing," in *Proc. ACM Symposium on Operating Systems Principles (SOSP)*, 2011, pp. 249–264.

[19] M. Abadi, M. Burrows, B. Lampson, and G. Plotkin, "A calculus for access control in distributed systems," *ACM Transactions on Programming Languages and Systems*, vol. 15, no. 4, pp. 706–734, Sep. 1993.

[20] J. Howell, "Naming and sharing resources across administrative domains," Ph.D. dissertation, Dartmouth College, 2000.

[21] D. Garg and M. Abadi, "A modal deconstruction of access control logics," in *Proc. Conference on Foundations of Software Science and Computational Structures (FOSSACS)*, 2008, pp. 216–230.

[22] V. Genovese, D. Garg, and D. Rispoli, "Labeled sequent calculi for access control logics: Countermodels, saturation and abduction," in *Proc. IEEE Computer Security Foundations Symposium (CSF)*, 2012, pp. 139–153.

[23] S. Kripke, "A semantical analysis of modal logic I: Normal modal propositional calculi," *Zeitschrift für Mathematische Logik und Grundlagen der Mathematik*, vol. 9, pp. 67–96, 1963, announced in *Journal of Symbolic Logic*, 24:323, 1959.

[24] G. E. Hughes and M. J. Cresswell, *A New Introduction to Modal Logic*. London: Routledge, 1996.

[25] R. Fagin, J. Y. Halpern, Y. Moses, and M. Y. Vardi, *Reasoning About Knowledge*. Cambridge, Massachusetts: MIT Press, 1995.

[26] R. A. Eberle, "A logic of believing, knowing and inferring," *Synthese*, vol. 26, pp. 356–382, 1974.

[27] R. Moore and G. Hendrix, "Computational models of beliefs and the semantics of belief structures," Technical Note 187, SRI International, 1979.

[28] M. Abadi, "Access control in a core calculus of dependency," *Electronic Notes in Theoretical Computer Science*, vol. 172, pp. 5–31, Apr. 2007.

[29] F. B. Schneider, K. Walsh, and E. G. Sirer, "Nexus authorization logic (NAL): Design rationale and applications," *ACM Transactions on Information and System Security*, vol. 14, no. 1, pp. 8:1–28, Jun. 2011.

[30] A. S. Troelstra and D. van Dalen, *Constructivism in Mathematics: Volume I*, ser. Studies in Logic and the Foundations of Mathematics. Amsterdam: Elsevier, 1988, vol. 121.

[31] ——, *Constructivism in Mathematics: Volume II*, ser. Studies in Logic and the Foundations of Mathematics. Amsterdam: Elsevier, 1988, vol. 123.

[32] D. Garg and F. Pfenning, "Non-interference in constructive authorization logic," in *Proc. IEEE Computer Security Foundations Workshop (CSFW)*, 2006, pp. 283–296.

[33] D. Wijesekera, "Constructive modal logics I," *Annals of Pure and Applied Logic*, vol. 50, no. 3, pp. 271–301, Dec. 1990.

[34] A. K. Simpson, "The proof theory and semantics of intuitionistic modal logic," Ph.D. dissertation, University of Edinburgh, 1994.

[35] R. Parikh, "Knowledge and the problem of logical omniscience," in *Proc. Int'l Symposium on Methodologies for Intelligent Systems (ISMIS)*, 1987, pp. 432–439.

[36] R. Stalnaker, "The problem of logical omniscience, I," *Synthese*, vol. 89, pp. 425–440, 1991.

[37] K. Konolige, *A Deduction Model of Belief*. Los Altos, California: Morgan Kaufmann, 1986.

[38] M. Abadi, "Variations in access control logic," in *Proc. Conference on Deontic Logic in Computer Science (DEON)*, 2008, pp. 96–109.

[39] J. Hintikka, *Knowledge and Belief*. Ithaca, New York: Cornell University Press, 1962.

[40] G. Plotkin and C. Stirling, "A framework for intuitionistic modal logics," in *Proc. Conference on Theoretical Aspects of Reasoning about Knowledge (TARK)*, 1986, pp. 399–406.

[41] G. Fischer Servi, "Semantics for a class of intuitionistic modal calculi," in *Italian Studies in the Philosophy of Science*, M. L. D. Chiara, Ed. Dordrecht, Holland: D. Riedel Publishing Company, 1981, pp. 59–72.

[42] W. B. Ewald, "Intuitionistic tense and modal logic," *Journal of Symbolic Logic*, vol. 51, no. 1, pp. 166–179, 1986.

[43] M. H. Sørensen and P. Urzyczyn, *Lectures on the Curry-Howard Isomorphism*, ser. Studies in Logic and the Foundations of Mathematics. Amsterdam: Elsevier, 2006, vol. 149.

[44] D. van Dalen, *Logic and Structure*, 4th ed. Berlin: Springer, 2004.

[45] S. Negri and J. von Plato, "Sequent calculus in natural deduction style," *Journal of Symbolic Logic*, vol. 66, pp. 1803–1816, 2001.

[46] B. F. Chellas, *Modal Logic: An Introduction*. Cambridge, United Kingdom: Cambridge University Press, 1980.

[47] R. Hakli and S. Negri, "Does the deduction theorem fail for modal logic?" *Synthese*, vol. 187, no. 3, pp. 849–867, 2012.

[48] D. Garg and F. Pfenning, "Stateful authorization logic: Proof theory and a case study," in *Proc. Conference on Security and Trust Management (STM)*, 2011, pp. 210–225.

[49] E. Moggi, "Notions of computation and monads," *Journal of Information and Computation*, vol. 93, no. 1, pp. 55–92, Jul. 1991.

APPENDIX A
PROOFS

Proposition 1.

Proof: By structural induction on ϕ. This proof has been mechanized in Coq. ■

Proposition 2.

Proof: Let $B = k2b(K)$. For B to be well-formed it must satisfy several conditions, which were defined in §II. We now show that these hold for any such B constructed by $k2b$.

1) Worldview Montonicity. Assume $w \leq w'$ and $\phi \in \omega(w, p, v)$. By the latter assumption and the definition of $k2b$, we have that $K, w, v \models \hat{p}$ says ϕ. From proposition 1, it follows that $K, w', v \models \hat{p}$ says ϕ. By the definition of $k2b$, it then holds that $\phi \in \omega(w', p, v)$. Therefore $\omega(w, p, v) \subseteq \omega(w', p, v)$.
2) Principal Equality (Belief). Assume $p \doteq p'$. Then by Principal Equality (Kripke), $\leq_p$ equals $\leq_{p'}$. By the Kripke semantics of $\mathsf{speaksfor}$, it follows that $K, w, v \models p$ says ϕ iff $K, w, v \models p'$ says ϕ. By the definition of $k2b$, therefore, $\omega(w, p, v) \subseteq \omega(w, p', v)$.
3) Deductive Closure. Assume $\Gamma \vdash \phi$. By rule SAYS-LRI, we have p says $\Gamma \vdash p$ says ϕ. By theorem 3, the following fact follows:[26] if, for all $\psi \in \Gamma$, it holds that $K, w, v \models p$ says ψ, then it also holds that $K, w, v \models p$ says ϕ. Assume $\Gamma \subseteq \omega(w, p, v)$. Then for all $\psi \in \Gamma$, it holds that $\psi \in \omega(w, p, v)$. By the definition of $k2b$, for all $\psi \in \Gamma$, it follows that $K, w, v \models \hat{p}$ says ψ. Therefore, by the fact we previously established, $K, w, v \models p$ says ϕ. By the definition of $k2b$, we have $\phi \in \omega(w, p, v)$.
4) Says Transparency. We prove the "iff" by proving both directions independently. ($\Rightarrow$) Assume $\phi \in \omega(w, p, v)$ and $p = \mu(\tau)$. By the definition of $k2b$, it holds that $K, w, v \models \tau$ says ϕ. From IT and F2, it follows that $K, w, v \models \tau$ says (τ says ϕ). By the definition of $k2b$, therefore, (τ says ϕ) $\in \omega(w, p, v)$. ($\Leftarrow$) Assume (τ says ϕ) $\in \omega(w, p, v)$ and $p = \mu(\tau)$. By the definition of $k2b$, it holds that $K, w, v \models \tau$ says (τ says ϕ). From ID, it follows that $K, w, v \models \tau$ says ϕ. By the definition of $k2b$, therefore, $\phi \in \omega(w, p, v)$.
5) Hand-off. Assume τ' $\mathsf{speaksfor}$ $\tau \in \omega(w, \mu(\tau), v)$. By the definition of $k2b$, it holds that $K, w, v, \models \tau$ says (τ' $\mathsf{speaksfor}$ τ). Expanding the semantic definition of says, we have that, for all w' and w'' such that $w \leq w' \leq_{\mu(\tau)} w''$, it holds that $K, w'', v \models \tau'$ $\mathsf{speaksfor}$ τ. Expanding the semantic definition of $\mathsf{speaksfor}$, we have that $\mathit{ReachAcc}(\mu(\tau'), w'') \supseteq \mathit{ReachAcc}(\mu(\tau), w'')$. By the definition of $\mathit{ReachAcc}$, we have the following fact: $\mathit{ReachAcc}(\mu(\tau'), w') \supseteq \mathit{ReachAcc}(\mu(\tau), w')$. Assume $\phi \in \omega(w, \mu(\tau'), v)$. By the definition of $k2b$, it holds that $K, w, v \models \tau'$ says ϕ. Expanding the semantic definition of says, we have that, for all w' and w'' such that $w \leq w' \leq_{\mu(\tau')} w''$, it holds that $K, w'', v \models \phi$. Now consider any w''' such that $w' \leq_{\mu(\tau)} w'''$. From the fact we previously established, it follows that $w' \leq_{\mu(\tau')} w'''$. One such w''' is w'' itself, so we have $w' \leq_{\mu(\tau')} w''$. We can then conclude for all w' and w'' such that $w \leq w' \leq_{\mu(\tau)} w''$, it holds that $K, w'', v \models \phi$. By the semantic definition of says, we have that $K, w, v \models \tau$ says ϕ holds. By the definition of $k2b$, it holds that $\phi \in \omega(w, \mu(\tau), v)$. Therefore $\omega(w, \mu(\tau'), v) \subseteq \omega(w, \mu(\tau), v)$.

■

Theorem 1.

Proof: By structural induction on ϕ. All of the cases except says and $\mathsf{speaksfor}$ are straightforward, because those are the only two cases where the interpretation of formulas differs in the two semantics.

- Case $\phi = \tau$ says ψ. Suppose $K, w, v \models \tau$ says ψ. By the definition of $k2b$, formula $\psi \in \omega(w, \mu(\tau), v)$. By the belief semantics of says, it must hold that $k2b(K), w, v \models \tau$ says ψ.
- Case $\phi = \tau$ $\mathsf{speaksfor}$ τ'. Suppose $K, w, v \models \tau$ $\mathsf{speaksfor}$ τ'. Consider any ψ in $\omega(w, \mu(\tau), v)$. By the definition of $k2b$, it holds that $K, w, v \models \tau$ says ψ. From the Kripke semantics of says and $\mathsf{speaksfor}$, it follows that $K, w, v \models \tau'$ says ψ. By the definition of $k2b$, it thus also holds that $\psi \in \omega(w, \mu(\tau'), v)$. So for all ψ, if $\psi \in \omega(w, \mu(\tau), v)$, then $\psi \in \omega(w, \mu(\tau'), v)$. Thus $\omega(w, \mu(\tau), v) \subseteq \omega(w, \mu(\tau'), v)$. By the belief semantics of $\mathsf{speaksfor}$, it therefore holds that $k2b(K), w, v \models \tau$ $\mathsf{speaksfor}$ τ'.

■

Lemma 1. $B, w, v \models \tau$ says Γ implies $\Gamma \subseteq \omega(w, \mu(\tau), v)$.

Proof: Assume $B, w, v \models \tau$ says Γ. By the semantics of says, we have that for all $\psi \in \Gamma$, it holds that $\psi \in \omega(w, \mu(\tau), v)$, hence $\Gamma \subseteq \omega(w, \mu(\tau), v)$. ■

Theorem 2.

Proof: By induction on the derivation of $\Gamma \vdash \phi$. All of the cases except those involving says and $\mathsf{speaksfor}$ are routine. Let $B, w, v \models \Gamma$ denote that, for all $\psi \in \Gamma$, it holds that $B, w, v \models \psi$.

1) SAYS-LRI. Assume that $\Gamma \vdash \phi$. We need to show that $B, w, v \models \tau$ says Γ implies $B, w, v \models \tau$ says ϕ. So assume $B, w, v \models \tau$ says Γ. By Lemma 1, $\Gamma \subseteq \omega(w, \mu(\tau), v)$. By Deductive Closure, $\phi \in \omega(w, \mu(\tau), v)$. Therefore, by the semantics of says, we have $B, w, v \models \tau$ says ϕ.
2) SAYS-LI. Assume that $\Gamma \vdash \tau$ says ϕ. We need to show that $B, w, v \models \tau$ says Γ implies $B, w, v \models \tau$ says ϕ. So assume $B, w, v \models \tau$ says Γ. By Lemma 1, $\Gamma \subseteq \omega(w, \mu(\tau), v)$. By Deductive Closure, τ says $\phi \in \omega(w, \mu(\tau), v)$. By Says Transparency, $\phi \in \omega(w, \mu(\tau), v)$. Therefore, by the semantics of says, $B, w, v \models \tau$ says ϕ.
3) SAYS-RI. Assume that τ says $\Gamma \vdash \phi$. We need to show that $B, w, v \models \tau$ says Γ implies $B, w, v \models \tau$ says ϕ. So assume $B, w, v \models \tau$ says Γ. By Lemma 1, $\Gamma \subseteq \omega(w, \mu(\tau), v)$. By Says Transparency, (τ says Γ) $\subseteq \omega(w, \mu(\tau), v)$. By Deductive Closure,

[26] Although this is a forward reference to a theorem we haven't proved yet, that theorem does not rely on the current proposition, so there is no circularity.

$\phi \in \omega(w, \mu(\tau), v)$. Therefore, by the semantics of says, $B, w, v \models \tau$ says ϕ.

4) SF-I. We need to show that $B, w, v \models \Gamma$ implies $B, w, v \models \tau_1$ speaksfor τ_2. Assume $B, w, v \models \Gamma$. Also assume that $\Gamma \vdash \tau_2$ says (τ_1 speaksfor τ_2). By the inductive hypothesis, if $B, w, v \models \Gamma$, then $B, w, v \models \tau_2$ says (τ_1 speaksfor τ_2). Thus $B, w, v \models \tau_2$ says (τ_1 speaksfor τ_2). By the semantics of says, we have τ_2 says (τ_1 speaksfor τ_2) $\in \omega(w, \mu(\tau_2), v)$. By Hand-off, $\omega(w, \mu(\tau_1), v) \subseteq \omega(w, \mu(\tau_2), v)$. By the semantics of speaksfor, $B, w, v \models \tau_1$ speaksfor τ_2 holds.
5) SF-E. We need to show that $B, w, v \models \Gamma$ implies $B, w, v \models \tau_2$ says ϕ. So assume $B, w, v \models \Gamma$. Also assume that $\Gamma \vdash \tau_1$ speaksfor τ_2 and $\Gamma \vdash \tau_1$ says ϕ. By the inductive hypothesis, if $B, w, v \models \Gamma$, then $B, w, v \models \tau_1$ speaksfor τ_2 and $B, w, v \models \tau_1$ says ϕ. So $B, w, v \models \tau_1$ speaksfor τ_2 and $B, w, v \models \tau_1$ says ϕ. By the semantics of speaksfor and says, we have $\omega(w, \mu(\tau_1), v) \subseteq \omega(w, \mu(\tau_2), v)$ and $\phi \in \omega(w, \mu(\tau_1), v)$. Thus $\phi \in \omega(w, \mu(\tau_2), v)$. Therefore, by the semantics of says, $B, w, v \models \tau_2$ says ϕ.
6) SF-R. Straightforward from the reflexivity of $\subseteq$ on worldviews.
7) SF-T. Straightforward from the transitivity of $\subseteq$ on worldviews.

■

Theorem 3.

Proof: This theorem is actually a corollary of theorem 5, because FOCALE generalizes FOCAL. ■

Theorem 4.

Proof: By induction on the derivation of $\Gamma \vdash \phi$. The proof generalizes the proof of theorem 2. The only interesting, new cases are for subprincipals and group principals:

1) MEMBER. We need to show that if $B, w, v \models \Gamma$, then $B, w, v \models \tau$ speaksfor $\{x : \phi\}$. So assume $B, w, v \models \Gamma$. Also assume that $\Gamma \vdash \phi[\tau/x]$. By the inductive hypothesis, if $B, w, v \models \Gamma$ then $B, w, v \models \phi[\tau/x]$. So we have $B, w, v \models \phi[\tau/x]$. Therefore τ satisfies the characteristic predicate defining group $\{x : \phi\}$. By definition, $\mu(\{x : \phi\}) = \bigsqcup\{p \mid B, w, v[p/x] \models \phi\}$. One of the principals p in that join must be $\mu(\tau)$. So $\mu(\{x : \phi\}) = \mu(\tau) \sqcup \bigsqcup\{p \mid B, w, v[p/x] \models \phi\}$. Let $\Pi = \bigsqcup\{p \mid B, w, v[p/x] \models \phi\}$. Then we have $\mu(\{x : \phi\}) = \mu(\tau) \sqcup \Pi$; call this Fact 1. Consider $\omega(w, \mu(\{x : \phi\}), v)$. We can rewrite it, using Fact 1, as $\omega(w, \mu(\tau) \sqcup \Pi, v)$. By Group Principal (Belief), that can be rewritten as the deductive closure of $\omega(w, \mu(\tau), v) \cup \omega(w, \Pi, v)$. Again using Fact 1, we can rewrite that as the deductive closure of $\omega(w, \mu(\tau), v) \cup \omega(w, \Pi, v)$. So, following that chain of rewriting, we have that $\omega(w, \mu(\{x : \phi\}), v)$ equals the deductive closure of $\omega(w, \mu(\tau), v) \cup \omega(w, \Pi, v)$. Since taking the deductive closure can only add formulas, never remove them, it follows that $\omega(w, \mu(\tau), v) \subseteq \omega(w, \mu(\{x : \phi\}), v)$. Therefore, by the semantics of speaksfor, we have that $B, w, v \models \tau$ speaksfor $\{x : \phi\}$.
2) SF-GROUP. We need to show that $B, w, v \models \Gamma$ implies $B, w, v \models \{x : \phi\}$ speaksfor τ. So assume that $B, w, v \models \Gamma$. Also assume that $\Gamma, \phi \vdash x$ speaksfor τ, and that $x \notin FV(\tau) \cup FV(\Gamma)$. By the inductive hypothesis, we have that if $B, w, v \models \Gamma, \phi$ then $B, w, v \models x$ speaksfor τ. But since we already have $B, w, v \models \Gamma$, it follows that $B, w, v \models \phi$ implies $B, w, v \models x$ speaksfor τ. Note that $B, w, v \models \phi$ holds whenever v maps x to a principal of which characteristic predicate ϕ holds. Call that principal p. Then whenever ϕ holds of p, it also holds that $B, w, v \models \hat{p}$ speaksfor τ, hence by the semantics of speaksfor, that $\omega(w, p, v) \subseteq \omega(w, \mu(\tau), v)$. Let $\Pi = \mu(\{x : \phi\}) = \bigsqcup\{p \mid B, w, v[p/x] \models \phi\}$. By Group Principal (Belief), worldview $\omega(w, \Pi, v)$ is the deductive closure of $\bigcup_{p \in \Pi} \omega(w, p, v)$. Since for all $p \in \Pi$, characteristic predicate ϕ holds of p, it follows that $\omega(w, p, v) \subseteq \omega(w, \mu(\tau), v)$. Let $W_\Pi = \left(\bigcup_{p \in \Pi} \omega(w, p, v)\right)$. Thus $W_\Pi \subseteq \omega(w, \mu(\tau), v)$. The deductive closure of W_Π is $\omega(w, \Pi, v)$. Are there any formulas in $\omega(w, \Pi, v)$ that are not in $\omega(w, \mu(\tau), v)$? Consider $\psi \in \omega(w, \Pi, v)$, such that $\psi \notin \bigcup_{p \in \Pi} \omega(w, p, v)$. Then there must be $\Gamma \subseteq \bigcup_{p \in \Pi} \omega(w, p, v)$, such that $\Gamma \vdash \psi$. But since $\Gamma \subseteq \bigcup_{p \in \Pi} \omega(w, p, v) \subseteq \omega(w, \mu(\tau), v)$, it must be that $\psi \in \omega(w, \mu(\tau), v)$, because $\omega(w, \mu(\tau), v)$ is a worldview hence is deductively closed. Thus, we have $\omega(w, \Pi, v) \subseteq \omega(w, \mu(\tau), v)$. By the semantics of speaksfor, we have $B, w, v \models \{x : \phi\}$ speaksfor τ.
3) SF-SUBPRIN. By the semantics of speaksfor, we must show that $\omega(w, \mu(\tau_1), v) \subseteq \omega(w, sub_w(\mu(\tau_1), \mu(\tau_2)), v)$ holds. This follows immediately from the definition of sub_w.

■

Theorem 5.

Proof: By induction on the derivation of $\Gamma \vdash \phi$. This proof has been mechanized in Coq. ■